Amendments to the Specification:

Please replace the indicated paragraphs with the following amended paragraph(s):

[0010] Protecting information systems from various forms of attack has long been of concern to practitioners in the field. Some forms of protection are built into operating systems, such as user and/or password authentication. Other forms of protection include various software and sometimes hardware strategies. A very commonly used form of protection is anti-virus software. Inventor Fred Cohen, as early as 1988, proposed and implemented an integrity shell, which was a program that run in an operating system kernel space and used a modified execution system call to verify a check sum over every program before executing that program. Such a modified system call allowed the system to protect against viruses that hid within executable components, because the presence of such viruses would change the checksum of those executable components. Further information about this work is available at http://~~all.~~all(.)net/books/integ/vmodels.html.

[0011] It is believed to be generally known to modify parts of an operating system, including parts of kernel system calls, for various reasons. In some cases, modified system calls will preserve original system calls in order to remove modifications or in order to run original system calls after the modified portion is run. For example, such techniques are discussed in "The Linux Kernel Module Programming Guide" by Ori Pomerantz, believed available 1999-05-19. (see ~~www.~~www(.)tldp.~~org~~(.)org/LDP/lkmpg/node20.html.)

[0012] Various strategies used in computer systems have at times included providing some type of misinformation. Some logic modules, for example, are designed to hide themselves from various operating system functions, such as process viewing functions, and thus can cause functions to provide a list of processes and/or files and/or users, for example, that are not complete. One use of such a strategy is mentioned in the context of a program referred to as the Kernel Intrusion System. This program is described as a kernel level rootkit that, among other things, makes modifications to the kernel to get some privileges, and hides itself from system administrators. Further information is available at ~~www.~~www(.)packetstormsecurity.~~org~~(.)org/UNIX /penetration/ rootkits/kis-0.9.tar.gz.

Other References

1. Fred Cohen, Operating System Protection Through Program Evolution, Computers and Security 1992. (In this paper, techniques for automatically modifying programs without changing their operation are given as a method of camouflage to conceal points of attack.) ~~all.~~all(.)net/books/IP/evolve.html
2. Fred Cohen, Information System Defenses - A Preliminary Classification Scheme Computers and Security, 1997. (This paper describes almost 140 different classes of protective methods gathered from many different sources.) ~~all.~~all(.)net/CID/Defense/Defense.xref
3. Fred Cohen et. al. Model-Based Situation Anticipation and Constraint
4. Fred Cohen, Algorithmic Authentication of Identification, Information Age, V7#1 (Jan. 1985), pp 35-41.
5. Fred Cohen, A Note on Detecting Tampering with Audit Trails, IFIP-TC11, `Computers and Security', 1996 ~~all.~~all(.)net/books/audit/audmod.html
6. W. Cheswick and S. Bellovin, Firewalls and Internet Security - Repelling the Wiley Hacker Addison-Wesley, 1994.
7. Mikhail Auguston, J. Bret Michael, Richard Riehle, and Neil C. Rowe, "Software Decoys: Intrusion Detection and Countermeasures," Proceedings of the 2002 IEEE Workshop on Information Assurance, West Point, NY, June 2002. ~~www.~~www(.)cs.nps.navy.mil/people/faculty/bmichael/publications.html.
8. Mikhail Auguston, Georgios Fragkos, and J. Bret Michael, "An Experiment in Software Decoy Design: Intrusion Detection and Countermeasures via System Call Instrumentation," Proceedings of the IFIP 18th International Information Security Conference, Athens, Greece, May 2003. ~~www.~~www(.)cs.nps.navy.mil/people/faculty/bmichael/publications.html.
9. Fred Cohen, "A Note on the Role of Deception in Information Protection," ~~all.~~all(.)net/journal/deception/deception.html, 1998.
10. Fred Cohen, Irwin Marin, Jeanne Sappington, Corbin Stewart, and Eric Thomas, "Red Teaming Experiments with Deception Technologies," ~~all.~~all(.)net/journal/deception/experiments/experiments.html, November 2001.
11. Harold S. Javitz and Alfonso Valdes, The NIDES Statistical Component Description and Justification, Annual Report, A010, March 1994.
12. James Bret Michael and Richard D. Riehle, "Intelligent Software Decoys," Proceedings of the Monterey Workshop on Engineering Automation for Software-Intensive System Integration,

Monterey, CA, June 2001. ~~www.~~www(.)cs.nps.navy.mil/people/faculty/bmichael/pubs/decoys-mtyworkshop2001.pdf.

13. James Bret Michael, "On the Response Policy of Software Decoys: Conducting Software-Based Deception in the Cyber Battlespace," Proceedings of the 26th Annual Computer Software and Applications Conference, Oxford, England, August 2002. ~~www.~~www(.)cs.nps.navy.mil/people/faculty/bmichael/publications.html.
14. Lance Spitzner, "Honeypots: Definitions and Value of Honeypots," ~~www.~~www(.)trackinghackers.~~com~~(.)com/papers/honeypots.html, May 2003.